Filtrage par DNS

J-EOLE/J-SR

31 mai 2017

Nicolas Schont, Rectorat de Versailles

Problématique :

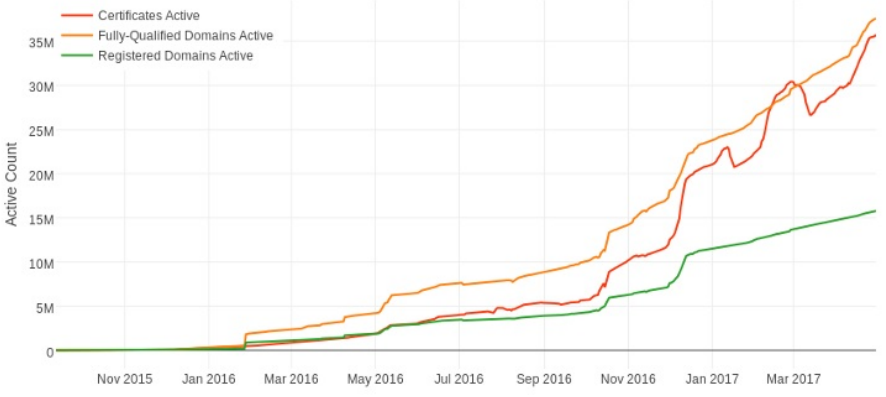
Écoles sans filtrage elles sont dans de petites communes, peu de postes de travail.

Proxy centralisé :

- Gestion de comptes
- Lenteur
- Bande passante du service central
- Proxy ICap, requiére soit une application locale soit un boitier mais utilise la bande passante du client
- Sites en HTTPS

Nombre de certificats let's encrypt

Forte augmentation des sites en HTTPS gràce à l'arrivée de **"let's encrypt"** porté entre par la fondation Mozilla, EFF



source : [letsencrypt]

Pourcentage de sites en HTTPS

Statistique pour Firefox

source : [letsencrypt]

Les nouveaux protocoles

rendent difficile voir impossible l'analyse des pages en HTTPS via du déchiffrement SSL (MITM)

- HTTP Strict Transport Security (HSTS) 2012 avec des options Preloading/subdomain
- Prévention contre les certificats frauduleux Pinning (HPKP) 2015
- Verification de la validé du certificat en Temps réels (OCSP stapling) 2013
- Autorité de certification pouvant valdider le cerficat (DNS CAA) 2013

Implémentation de OCSP chez M$

ce qu'il reste à regarder en HTTPS :

https://mondomain.fr/ ~~url_.html~~

bref il reste le FQDN

DNS Menteur

- DNSMASQ central 
  - 2 serveurs en *load balancer*

Partenariat avec Qwant

Qwant propose depuis 2015 d'un DNS menteur afin de procéder au filtrage de Qwant Junior :

- Qwant DNS

  171.33.77.129
  171.33.77.209
  Qwant intégre les listes de Toulouse comme celle du contenu Adulte

DNSMASQ Incorporation des

Listes de noires de Toulouse

- /etc/dnsmasq.d/
  - malware-domain-dns.conf
  - 02-acver-redirection.conf
  - dating-domain-dns.conf
  - marketingware-domain-dns.conf
  - tricheur-domain-dns.conf
  - ddos-domain-dns.conf
  - phishing-domain-dns.conf
  - warez-domain-dns.conf
  - 04-crypt.conf
  - drugs-domain-dns.conf
  - publicite-domain-dns.conf
  - agressif-domain-dns.conf
  - gambling-domain-dns.conf
  - arjel-domain-dns.conf
  - hacking-domain-dns.conf
  - redirector-domain-dns.conf

DNSMASQ Rewrite domaine

rewrite afin de forcer le *safe search* (bing, duckduckgo, google, qwant)

```
cname=google.com,forcesafesearch.google.com
cname=google.fr,forcesafesearch.google.com
cname=www.youtube.com,restrict.youtube.com
cname=m.youtube.com,restrict.youtube.com
cname=youtubei.googleapis.com,restrict.youtube.com
cname=youtube.googleapis.com,restrict.youtube.com
cname=www.youtube-nocookie.com,restrict.youtube.com
cname=www.bing.com,strict.bing.com
cname=bing.com,strict.bing.com
cname=duckduckgo.com,safe.duckduckgo.com
cname=qwant.com,safeapi.qwant.com
```

Améliorer la bande passante et de la sécurité sans intervention en local sur les matériels des écoles

- Ajout de liste de régies publicitaires en listes noires afin de limiter les piratages des pubs
- Ajout de sites malveillants comme récemment pour Wannacry

Mises à jours des configurations de DNSMASQ

- Ordonnanceur (récupération des listes et scripts de remise en forme)
- Gestion des versions des fichiers avec Gitlab

address=/03bbec4.netsolhost.com/194.187.168.102
address=/0551fs.com/194.187.168.102
address=/0571jjw.com/194.187.168.102
address=/07353.com/194.187.168.102
address=/0743j.com/194.187.168.102

ce que cela pose comme soucis

- log : on a les sites demandés et l'IP publique qui l'a demandé, mais chez certain FAI l'IP n'est pas fixe

  Piste :

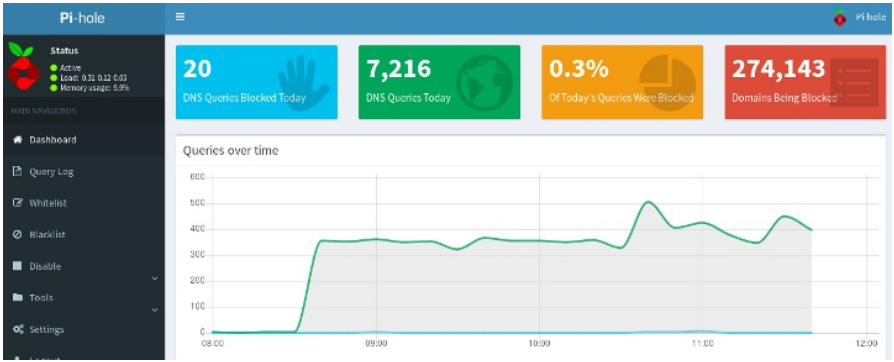
  - Les FAI progressent sur le déploiement de l'IPv6
    - Orange 16%
    - Free 28% (+4% en 4 mois)
  - on pourrait donc avoir l'IP du poste en IPv6

- il est possible d'utiliser l'IP pour naviguer (vs fqdn) mais avec les CDN (cloudflare entre autre) beaucoup de sites ne seront pas joignable

un interface

pour voir rapidement de quoi il retourne

- Pihole



QUESTIONS ?